

Report summary

GGUF v3 model | quantization: Mixed/Unknown | 0 tensors | 1 blocking issue / 3 warnings

Model

Filename	malformed-kv-length.gguf
Format	gguf
Architecture	—
Size	69 B
SHA-256	c22d91c6e53a1848f4ef32abdaf1ac46102c9caf035b18a0d1f3402dc32541dc
Scan mode	static-deep
Scanned at	2026-08-10T20:47:49+00:00Z
Report ID	4be504239c1d497ba76013d981606e28

Findings (4)

SEVERITY	CATEGORY	DETAIL
HIGH	Parse	KV metadata decode error str bytes Recommendation: File may be truncated or malformed; re-download from source
LOW	Metadata	Missing general.architecture key Cannot determine model architecture without this field Recommendation: Verify model provenance; request metadata from the model provider
LOW	Supply Chain	No license field in GGUF metadata (general.license) Absence of license information makes it impossible to determine usage rights Recommendation: Add general.license to model metadata before distributing; use an SPDX identifier
LOW	Supply Chain	No embedded provenance metadata None of general.author, general.source.url, general.base_model.0, or general.source.huggingface.repository are embedded in the GGUF file. Without any origin signal the model cannot be traced to a trusted source or compared against a reference checkpoint for tampering detection. For files uploaded directly, provenance is especially critical because the scanner cannot infer repository origin from the file alone. Recommendation: Add at least one of: general.author, general.source.huggingface.repository, or general.source.url

Runtime compatibility

RUNTIME	SUPPORTED	NOTES
llama.cpp	No	GGUF v3 container: supported quant Mixed/Unknown: supported — architecture unknown, cannot assess support
Ollama	No	

GGUF via llama.cpp backend: container and quantization supported — architecture unknown, cannot assess support

LM Studio	No	GGUF container and quantization supported; GPU/CPU inference — architecture unknown, cannot assess support
vLLM	No	GGUF not supported; requires safetensors format
HuggingFace Transformers	No	GGUF not supported; requires safetensors or PyTorch checkpoint

Generated 2026-08-21 06:50 UTC by LLMScan.online (engine v2.0.0, report schema v1.0). Full interactive report: <https://llmscan.online/report/4be504239c1d497ba76013d981606e28> — Static analysis only; not a guarantee of safety. See llmscan.online/docs/how-it-works for methodology.